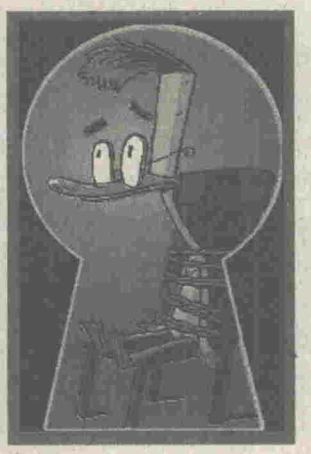
■ กองบรรณาธิการ

IT SECURITY
Computer - Network
Security and Information Protection



นโยบายและการดูแลรักษาระบบในองค์กร

นโยบายและการดูแลรักษาระบบ
และความปลอดภัยของข้อมูลในองค์กร
การหาทางป้องกันไว้ก่อนจะต้องกระทำ
และมีหนทางเตรียมการไว้อย่างชัดเจน

การใช้เทคโนโลยีสารสนเทศมีบทบาทและความจำเป็นสำหรับองค์กรมากขึ้น ทุกองค์กรมีการใช้คอมพิวเตอร์ ตั้งแต่พีซีแบบตั้งโต๊ะ เชื่อมโยงกันเป็นเครือข่ายในลักษณะเวิร์กกรุ๊ป และเชื่อมต่อเป็นอินทราเน็ตขององค์กร ตลอดจนเชื่อมโยงต่อเข้าสู่โลกภายนอกคืออินเทอร์เน็ต และเข้าสู่เครือข่ายบริการสาธารณะอื่น ๆ อีกหลายอย่าง

เมื่อเทคโนโลยีได้รับการพัฒนาให้ก้าวหน้ามากขึ้น ขบวนการในเรื่องอาชญากรรมและโจรกรรมในลักษณะการบุกรุกผ่านเข้ามาทางเครือข่ายก็มีมากขึ้น มีทั้งจากพวกที่ต้องการลองวิชา ลองของ ลองโปรแกรม หรือพวกนึกสนุก ตลอดจนพวกจิตวิปริต และพวกมิจฉาชีพต่าง ๆ ที่แทรกเข้ามาหาผลประโยชน์ต่าง ๆ

องค์กรทางธุรกิจ องค์กรที่ดำเนินการโดยใช้เครือข่ายสื่อสารและคอมพิวเตอร์ต่าง ๆ จึงต้องปรับตัวและหาทางป้องกัน เรียนรู้ ทำความเข้าใจในปัญหาที่อาจเกิดขึ้น เตรียมหาทางป้องกัน รวมทั้งการกำหนดนโยบายหลักให้ผู้ปฏิบัติงานต่าง ๆ ถือปฏิบัติ และหาทางป้องกัน รวมถึงการวางกฎระเบียบต่าง ๆ ขององค์กร

ผู้บริหารจะต้องให้ความสำคัญ

ปัญหาการใช้เทคโนโลยีในองค์กรยังมีจุดอ่อนหรือมีรูรั่วอยู่มาก ข้อมูลข่าวสารบางอย่างเป็นข้อมูลที่มีค่า และอาจทำให้องค์กรเสียหายได้มาก เช่น ในอดีตที่ผ่านมา มีบริษัทในต่างประเทศแห่งหนึ่ง เก็บข้อมูลลูกค้าที่ใช้โทรศัพท์มือถือและรหัสเครื่องที่สำคัญเอาไว้ที่เครื่องเซิร์ฟเวอร์ มีผู้บุกรุกเข้ามาคัดลอกข้อมูลนี้ไปได้ ทำให้สามารถนำไปใช้ในการจูนโทรศัพท์มือถือ ทำให้ลูกค้าจำนวนมากเดือดร้อน และสร้างความเสียหายให้ระบบอย่างมาก

ปัญหาเรื่องความปลอดภัยของข้อมูลข่าวสารและความปลอดภัยของระบบจึงเป็นเรื่องสำคัญเป็นเรื่องใหญ่ ในเกือบทุกองค์กรมีระบบการป้องกันแตกต่างกัน และทุกองค์กรต้องเสียเงินเสียทองไปกับระบบป้องกันเป็นจำนวนมาก มีการตั้งระบบตรวจสอบ ระบบไฟร์วอลล์ ติดตั้งซอฟต์แวร์เฉพาะ และยังสร้างความไม่สะดวกกับผู้ใช้ต่าง ๆ นานา จนผู้ใช้หลายคนรู้สึกถึงความยุ่งยากในการใช้งาน

นโยบายที่สำคัญขององค์กร

องค์กรทุกองค์กรจึงต้องกำหนดนโยบายที่สำคัญเกี่ยวกับเรื่องการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ดูแลรักษาความปลอดภัยทั้งของระบบและข้อมูล สิ่งที่สำคัญควรประกอบด้วย

- นโยบายหลักในเรื่องการให้ความสำคัญของระบบความปลอดภัยของข้อมูลข่าวสารและเครือข่ายคอมพิวเตอร์
- นโยบายเกี่ยวกับการให้ความสำคัญในเรื่องการป้องกันเหตุการณ์ เพื่อไม่ให้มีปัญหาเกิดขึ้น การป้องกันเป็นเรื่องที่เกี่ยวโยงกับการลงทุน
- นโยบายเกี่ยวกับการรายงานปัญหา ผลที่เกิดขึ้นเมื่อมีผู้บุกรุก การตรวจสอบระบบ การประสานงาน การแก้ไขปัญหาต่าง ๆ
- นโยบายความร่วมมือกับองค์กรอื่น หรือแม้แต่องค์กรทางด้านการรักษาความสงบ เช่น ตำรวจ เพื่อให้การดำเนินงานเป็นไปตามขั้นตอนและกระบวนการที่ถูกต้อง

การดำเนินการหลายอย่างในประเทศไทยยังขาดขั้นตอนหรือวิถีทางปฏิบัติที่ชัดเจน โดยเฉพาะองค์กรทางด้านตำรวจยังไม่มีหน่วยงานที่เข้ามารับผิดชอบหรือดูแลในเรื่องนี้โดยตรง องค์กรที่จะป้องกันปราบปรามจะต้องเกิดขึ้นอย่างแน่นอนในอนาคต

ข้อแนะนำในการดูแลรักษาระบบขององค์กร

ข้อแนะนำที่จะกล่าวถึงนี้เป็นข้อแนะนำทั่วไปที่ผู้ดูแลรักษาระบบควรปฏิบัติ โดยเฉพาะระบบคอมพิวเตอร์ที่ต่อเชื่อมกับเครือข่าย และมีโอกาสที่จะได้รับการบุกรุกโดยผู้ไม่หวังดี

ผู้ดูแลระบบจะต้องมีหน้าที่และแนวทางในการปฏิบัติงานที่ชัดเจน มีขอบเขตของการดำเนินงานที่ทราบขั้นตอนการทำงานได้ชัดเจน เช่น เมื่อตรวจพบว่ามีผู้บุกรุกเข้ามาในระบบแล้ว จะปฏิบัติตนเองหรือดำเนินการอะไรบ้าง จะต้องแจ้งให้ใครทราบได้บ้าง และรายงานผลการดำเนินการต่าง ๆ ให้กับใคร หรือรับมอบอำนาจจากผู้ใดให้เข้ามาทำงาน

องค์กรควรมีเอกสารกำหนดขั้นตอนการปฏิบัติงานให้ชัดเจน เพื่อว่าผู้ดูแลระบบหรือผู้เกี่ยวข้องจะได้รับทราบและถ้าหากเกิดเหตุการณ์ขึ้นจริง จะต้องกระทำอะไรบ้าง จะตัดสินใจได้ในระดับใด จะแก้ไขสถานการณ์หรือปรึกษาทางด้านกฎหมายกับใคร การดำเนินการในเรื่องเหล่านี้จะต้องมีข้อกำหนดและกฎระเบียบที่ชัดเจน

ตัวอย่างขั้นตอนเมื่อรับรู้ว่ามีผู้บุกรุกเข้าระบบในระดับซูเปอร์ยูสเซอร์หรือรูทได้

สิ่งแรกที่กระทำคือการแจ้งผู้เกี่ยวข้อง หรือผู้บริหารในสายงานที่รับผิดชอบ ถ้าองค์กรใดมีการกำหนดขั้นตอนวิธีการรายงานผล ก็ต้องรีบดำเนินการรายงานผลให้ผู้เกี่ยวข้องได้ทราบทันที

เมื่อรับรู้ในเรื่องปัญหา ผู้ดูแลระบบจะต้องรีบดำเนินการต่าง ๆ โดยทันที การดำเนินการในลักษณะที่ต้องมีแผนฉุกเฉินที่ได้เตรียมไว้ โดยเฉพาะอย่างยิ่งในส่วนที่จะกระทบกับการทำงานปกติ หรือการแก้ปัญหางานปกติ สิ่งที่จะต้องกระทำประกอบด้วย

1. การปลดเครื่องคอมพิวเตอร์ที่ได้รับผลกระทบจากการบุกรุกหรือถูกบุกรุกออกจากเครือข่าย อย่างไรก็ตาม การที่เครื่องหนึ่งได้รับการเจาะระบบอาจเป็นไปได้ว่าเครื่องอื่นในเครือข่ายจะมีผลกระทบด้วย เพราะผู้เจาะระบบอาจวางโปรแกรมประเภท sniffer ไว้ เพื่อทำการตรวจสอบระบบเครือข่าย และเก็บข้อมูลผู้ใช้อื่น

2. คัดลอกข้อมูลของเครื่องที่ถูกบุกรุก การกระทำที่ดีคือการคัดลอกทั้งหมด โดยถ้าหากเรามีฮาร์ดดิสก์ที่มีขนาดและชนิดเดียวกัน เราสามารถนำมาทำสำเนาไว้ได้ เช่น ในระบบเครื่องยูนิกซ์ใช้คำสั่ง dd

```
# dd if = /dev/sda of = /dev/sdb
```

หากสงสัยวิธีการใช้คำสั่ง dd สามารถขอดูได้จากคู่มือหรืออยู่ใน man ของระบบอยู่แล้ว

อย่างไรก็ตาม การทำสำเนาในระดับต่ำ คือสำเนาทั้งหมดให้เหมือนกัน มีหลายวิธี

จะวิเคราะห์ผู้บุกรุกได้อย่างไร

เมื่อปลดระบบออกมาจากเครือข่ายแล้ว เราสามารถนำข้อมูลหรือระบบทั้งหมดมาตรวจสอบได้ การตรวจสอบจะต้องกระทำอย่างละเอียดรอบคอบ วิเคราะห์หาการเปลี่ยนแปลง หารูปแบบหรือสัญญาณที่บ่งบอกวิธีการเจาะระบบ ดูการกำหนด config ของระบบ ดูการแก้ไขเปลี่ยนแปลงที่ผู้บุกรุกได้กระทำ การกระทำที่สำคัญจึงประกอบด้วย

1. ตรวจสอบไฟล์ระบบและไฟล์คอนฟิกว่ามีการแก้ไขหรือไม่ วิธีการตรวจสอบไฟล์ระบบเป็นเรื่องใหญ่ เพราะมีมาก จะต้องตรวจสอบการแก้ไขในรูปแบบบางอย่าง เช่น ใช้วิธีการเปรียบเทียบ cmp ใช้วิธีการตรวจสอบ checksum ด้วยคำสั่ง sum

● การตรวจสอบไฟล์ระบบจะต้องรวมถึงไฟล์ /etc/passwd ดูว่ามีเพิ่มเติมมาหรือไม่

● ตรวจสอบดูว่า /etc/inetd.conf มีการเปลี่ยนแปลงไปจากเดิมหรือไม่

● ตรวจสอบไฟล์ .rhost ที่ให้ยอมการเรียกจากที่ห่างไกลด้วยคำสั่ง rlogin, rsh, rexec โดยต้องดูในไฟล์ /etc/hosts.equiv หรือมีข้อมูลใน .rhost ที่ยอมให้ผู้ให้ login ได้

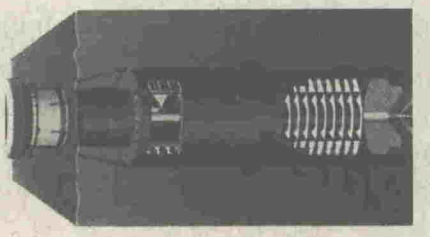
● ตรวจสอบว่ามี SUID และ SGID ใหม่เกิดขึ้นมาหรือไม่ เรามีคำสั่งที่พิมพ์ออกมา โดยใช้

```
#find /\(-perm -004000 -0 -perm -002000\) -type f -print
```

วิธีการค้นหาไฟล์นั้นต้องกระทำหมด เช่น หาไฟล์ที่เป็น ASCII ในไดเรคทอรี /dev ถ้ามีไดเรคทอรีสร้างขึ้นใหม่ให้สำรวจลงไปดูว่ามีไฟล์ซ่อนอยู่หรือไม่ บางครั้งไฟล์ที่ซ่อนมีลักษณะเป็นชื่อ... หรือ... ตามด้วยแบลงค์ทำให้หลอกตาได้

4. ตรวจสอบไฟล์ log ต่าง ๆ ทั้งหมด ในระบบมีไฟล์ log อยู่หลากหลาย เช่น ตรวจสอบดูใน /etc/syslog.conf

ในระบบยูนิกซ์มีไฟล์ log อยู่หลายแห่งและใช้ในการตรวจสอบเพื่อดูข้อมูลของผู้เข้าสู่ระบบ เช่น message, xferlog, utmp, wtmp, secure



2. ตรวจสอบดูการแก้ไขไฟล์ข้อมูล ข้อมูลที่อยู่ในระบบมักจะมีการแก้ไขโดยผู้บุกรุก ดังนั้นจึงควรตรวจสอบข้อมูลของทั้งระบบ เช่น ข้อมูลในเว็บเพจ ข้อมูลใน ftp ข้อมูลในโฮมไดเรคทอรี และข้อมูลในแฟ้มข้อมูลอื่น ๆ

3. ตรวจสอบดูเครื่องมือบางอย่างที่ผู้บุกรุกนำมาติดตั้งไว้ โปรแกรมหรือเครื่องมือที่ผู้บุกรุกนำมาติดตั้งมีมากมาย โปรแกรมเหล่านี้หาได้บนเครือข่ายอินเทอร์เน็ต และมีการพัฒนาใหม่เกิดขึ้นตลอดเวลา สิ่งที่สำคัญคือสามารถเปลี่ยนชื่อโปรแกรมและดัดแปลงแก้ไขกันต่อ ๆ ไปได้

โปรแกรมที่ผู้บุกรุกนิยม ได้แก่

● โปรแกรมตรวจสอบเครือข่าย (network sniffers) เป็นโปรแกรมที่คอยเก็บข้อมูลในเครือข่าย เช่น ชื่อผู้ login และ password

● โปรแกรมประเภทโทรจันฮอริส โปรแกรมพวกนี้ใช้ในการหลอกล่อหรือทำให้เข้าใจผิด ใช้ปกปิดเส้นทางการเข้าระบบ ใช้ในการเก็บข้อมูลระบบบางอย่าง

● โปรแกรมที่จะเปิดช่องทางให้ผู้บุกรุกเข้ามาในภายหลัง

● โปรแกรมที่ใช้ในการตรวจสอบระบบหรือตรวจสอบข้อมูลระบบในที่ห่างไกล รวมทั้งการเก็บข้อมูลผู้ใช้ที่ห่างไกลเพื่อต้องการความลับบางอย่าง

● โปรแกรมที่ดำเนินการเฉพาะอย่าง ซึ่งเราจะพบเห็นว่าโปรแกรมพวกนี้สร้างไฟล์ในลักษณะ log file เพื่อเก็บข้อมูลบางอย่างไว้ หรือส่งข้อมูลออกไปนอกระบบ

5. ตรวจสอบหลักฐานที่สร้างโดยโปรแกรม network sniffer โปรแกรมประเภท sniffer จะสร้าง log file ไว้ที่ใดที่หนึ่ง วิธีการที่จะตรวจสอบดูว่ามีโปรแกรมหรือโปรเซสใดใช้เน็ตเวิร์กอินเตอร์เฟสอยู่

การหาข้อมูลเกี่ยวกับการตรวจสอบและแก้ไขในเรื่องนี้ สามารถหาได้จาก

```
http://www.cert.org/advisories/CA-94.01.
ongoing.network.monitoring.attacks.html
```

6. ให้ตรวจสอบระบบอื่นที่เราดูแลในเครือข่ายด้วย จากประสบการณ์ที่ผ่านมาพบว่า หากมีเครื่องหนึ่งเครื่องใดถูกบุกรุก ผู้บุกรุกมักจะเข้าไปในเครื่องอื่น ๆ ด้วย ดังนั้นจึงจำเป็นต้องตรวจสอบเครื่องทุกเครื่องที่ต่ออยู่ในระบบเครือข่ายของเรา

7. ตรวจสอบดูการเชื่อมโยงไปยังเครื่องอื่นนอกระบบ ในการตรวจสอบไฟล์ log ต่าง ๆ เราจะพบการเชื่อมโยงไปยังเครื่องอื่น ๆ ทั้งจากเครื่องที่เป็นเครื่องต้นทางหรือเครื่องปลายทาง ผู้บุกรุกระบบส่วนใหญ่จะใช้เครื่องที่ตนเองเจาะผ่านมาก่อนเป็นการเข้าโจมตีเครื่องอื่น ดังนั้นเครื่องที่เชื่อมโยงที่ปรากฏในล็อกไฟล์ที่ผู้บุกรุกใช้มักจะเป็นเครื่องที่ถูกเจาะมาก่อนแล้ว

ศึกษาหาความรู้เป็นเรื่องสำคัญ

ผู้ดูแลระบบที่ดีจะต้องขยันและหมั่นศึกษาหาความรู้ ทั้งนี้เพราะวิธีการโจมตีระบบมีใหม่มาตลอดเวลา การศึกษาหาความรู้และเตรียมการไว้ก่อนเป็นเรื่องที่มีประโยชน์ต่อตนและองค์กรโดยตรง ปกติจะมีหน่วยงานรับแจ้งเหตุด่วนถึงวิธีการถูกโจมตีระบบ วิเคราะห์หาข้อมูลและเผยแพร่ให้ทราบ หน่วยงานนี้คือ CERT–Computer Emergency Response Team ซึ่งเป็นองค์กรรับแจ้งเหตุและกระจายข่าวสารให้กับผู้สนใจ CERT จะเป็นหน่วยงานที่รวบรวมข้อมูลข่าวสารต่าง ๆ ไว้มาก ผู้ดูแลรักษาระบบจึงควรหมั่นศึกษาจากเอกสารที่ CERT จัดทำขึ้น

การดำเนินการแก้ปัญหาที่สำคัญ

ในการดำเนินการภายในองค์กรจำเป็นต้องให้ความสำคัญ และถือว่าเป็นสิ่งที่ต้องปฏิบัติตาม โดยเฉพาะถ้าต้องการแก้ไขปัญหา จะต้องดำเนินการ

1. ติดตั้งโอเอสใหม่ เลือกโอเอสเวอร์ชันล่าสุด โดยเฉพาะตัวโปรแกรมที่มีการแก้ไขปัญหาต่าง ๆ แล้ว

2. ปิดบริการที่ไม่จำเป็นออกหมด เครื่องที่ใช้งานส่วนใหญ่มีบริการจำกัด ดังนั้นบริการที่ไม่จำเป็นจึงต้องปิดให้หมด เพราะบริการเหล่านั้นจะเป็นช่องทางเข้าสู่ระบบได้

3. ให้ติดตั้งแบตช์โปรแกรม ผู้ผลิตโอเอสมักจะมีโปรแกรมให้มาติดตั้งเพื่อแบตช์หรือแก้ไขปัญหาต่าง ๆ ของโอเอส ที่มีผู้ค้นพบภายหลัง ดังนั้นจึงควรรีบดำเนินการตามคำแนะนำ

4. ให้ทำตามคำแนะนำของ CERT CERT จะมีข้อสรุป ข้อเสนอแนะ มีคำแนะนำต่าง ๆ ให้ ดังนั้นจึงควรปฏิบัติตามหรือศึกษาดูว่าระบบยังมีจุดอ่อนที่ใด

5. ระมัดระวังการใช้ข้อมูลจากที่สำเนา เพราะการนำข้อมูลที่สำเนาออกมาใช้อาจทำให้โปรแกรมที่ผู้บุกรุกได้วางไว้กลับเข้ามาในระบบอีก

6. ให้เปลี่ยนรหัส password ของผู้ใช้ทุกคนในเครื่อง เพราะรหัสผ่านเก่าเป็นรหัสผ่านที่ไม่ปลอดภัยแล้ว

ความเคร่งครัดขององค์กร

องค์กรทุกองค์กรที่ต่อเครือข่ายคอมพิวเตอร์ของตนเองเข้าสู่เครือข่ายอินเทอร์เน็ตจะต้องระลึกเสมอว่าการบุกรุกจากบุคคลภายนอกจะเกิดขึ้นได้ตลอดเวลา การหาทางป้องกันไว้ก่อนจะต้องกระทำ และมีหนทางเตรียมการไว้อย่างชัดเจน เพราะระบบที่เราใช้อยู่ทุกระบบจะมีช่องโหว่ให้พวกมิจฉาชีพเข้ามาได้เสมอ

ดังนั้นหากระบบใดที่มีความสำคัญจึงต้องดูแลเป็นพิเศษ และไม่ควรนำต่อเข้ากับเครือข่ายสาธารณะ

ความเคร่งครัดในองค์กร โดยเฉพาะความร่วมมือในองค์กร ตั้งแต่การใช้รหัสผ่านที่ยากต่อการคาดเดา การใช้บริการบางอย่างที่เคารพกฎเกณฑ์ที่องค์กรวางไว้ รวมถึงการให้ความสำคัญ ช่วยเป็นหูเป็นตา แจ้งผู้แปลกปลอมหรือสงสัยในการบุกรุก โดยเฉพาะหากผู้ใช้ตรวจสอบดูว่าบัญชีชื่อของตนมีใครแอบอ้างเอาไปใช้บ้าง ก็จะตรวจสอบได้ในทุกครั้งที่ login เข้าไป เครื่องจะรายงานการใช้ครั้งก่อนหน้านี้

เอกสารอ้างอิง

1 http://www.cert.org/tech_tips/root_compromise/html
"Step for Recovering from UNIX Root Compromise"